
CYGNACOM
SOLUTIONS
an Entrust Technologies company

CYGNACOM SOLUTIONS
an Entrust Technologies company

Certification Path Development Software

Peter Hesse
Software Development Manager
pmhesse@cygnacom.com

Agenda

CYGNACOM SOLUTIONS
an Entrust Technologies company

- Overview of topologies and path development methods
- Discussion of CygnaCom's path development software
- Lessons learned developing and testing path development software
- Other path development software and development efforts

CYGNACOM SOLUTIONS
an Entrust Technologies company

Overview of Topologies and Path Development Methods

Definitions

CYGNACOM SOLUTIONS
an Entrust Technologies company

- Subscriber
  - End entity “certified” by a CA
- Trust root
  - Relying party trusts this and all entities which it has “certified”
- Certificate Path
  - Ordered list of certificates that connect a subscriber to a trust root

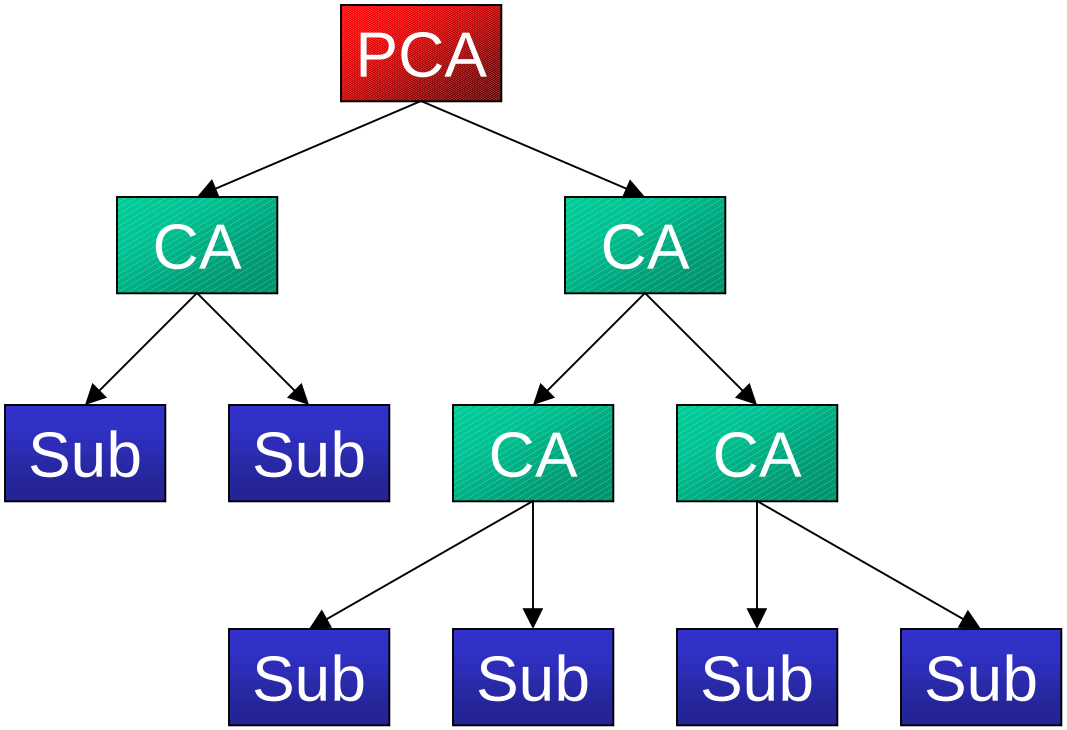
Trust Topologies

CYGNACOM SOLUTIONS
an Entrust Technologies company

- Many different PKI topologies are possible
- We'll discuss two that are easy to identify:
  - Hierarchy
  - Mesh
- Other topologies are typically a combination of those two

Hierarchy Topology

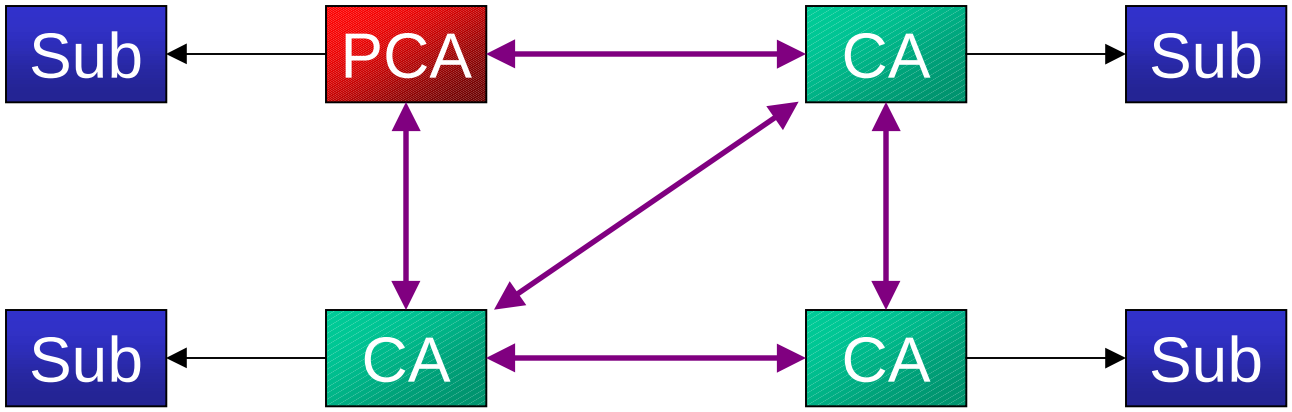
CYGNACOM SOLUTIONS
an Entrust Technologies company



- Trust root at “top”
- Certificate issuance always one-way “down”

Mesh Topology

CYGNACOM SOLUTIONS
an Entrust Technologies company

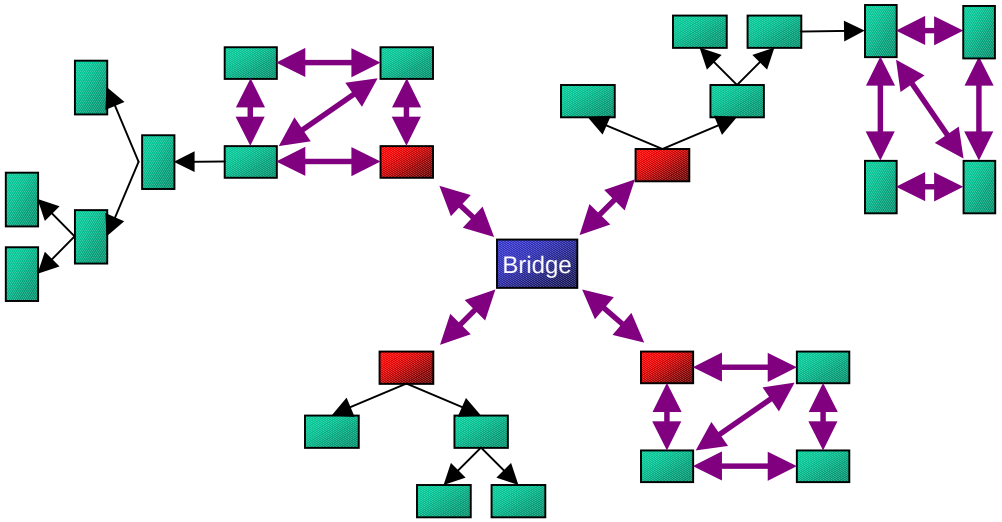


- Trust root depends on frame of reference (typically closest)
- CAs are cross-certified; subscribers have one-way issuance

Bridge CA Topology

CYGNACOM SOLUTIONS
an Entrust Technologies company

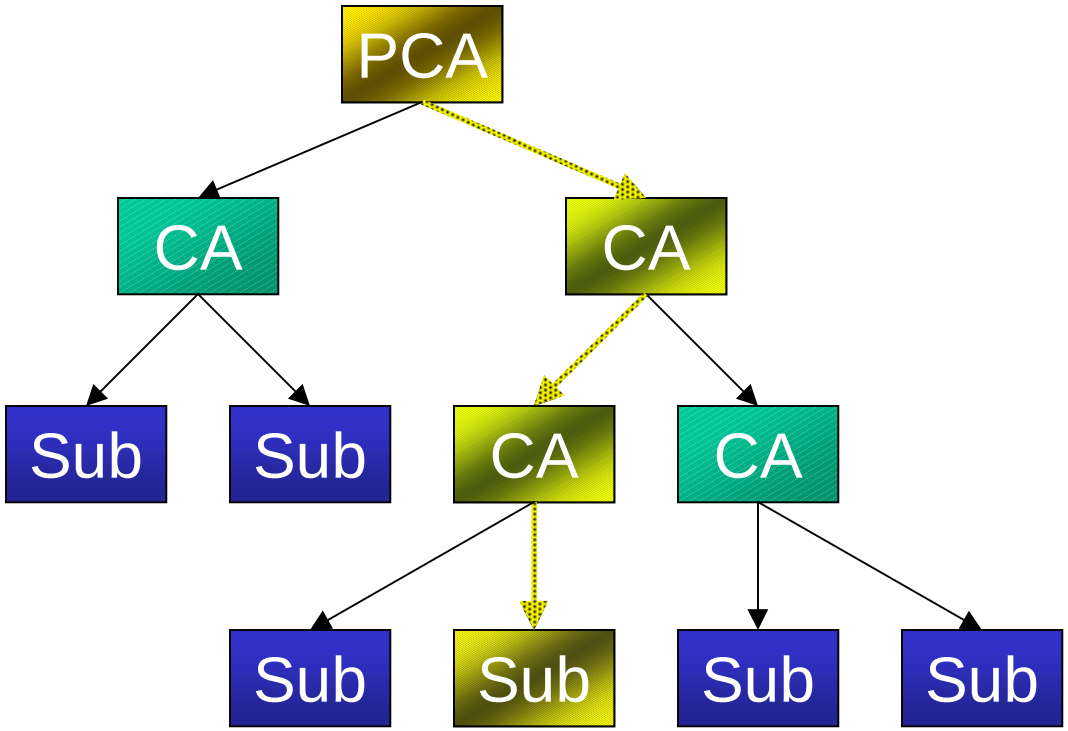
- The Bridge CA concept creates combinations of topologies which must be navigated by software



Developing Certificate Paths in a Hierarchy

CYGNACOM SOLUTIONS
an Entrust Technologies company

- In a hierarchy, there's only one way to go from the subscriber to the trust root: start at subscriber and follow the issuer.

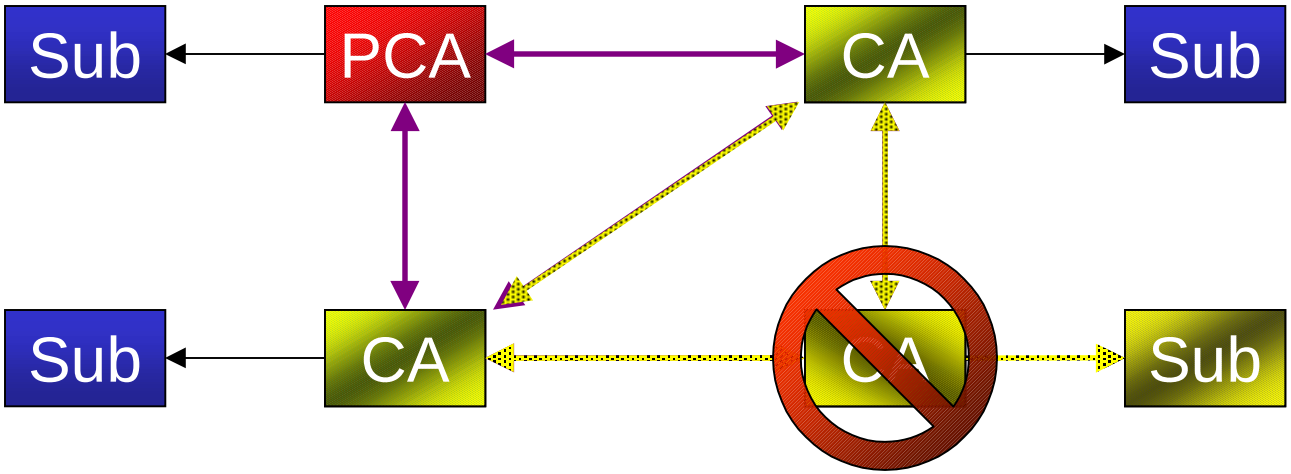


This slide is animated.

Developing Certificate Paths in a Mesh

CYGNACOM SOLUTIONS
an Entrust Technologies company

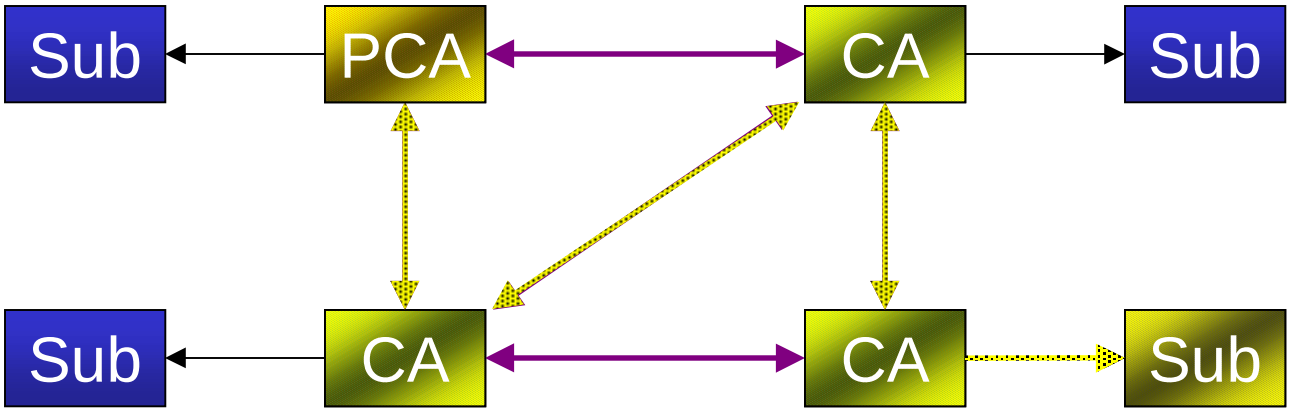
- In a mesh, it gets trickier… "follow the issuer" ends up with many choices.
- You might find loops…



Developing Certificate Paths in a Mesh

CYGNACOM SOLUTIONS
an Entrust Technologies company

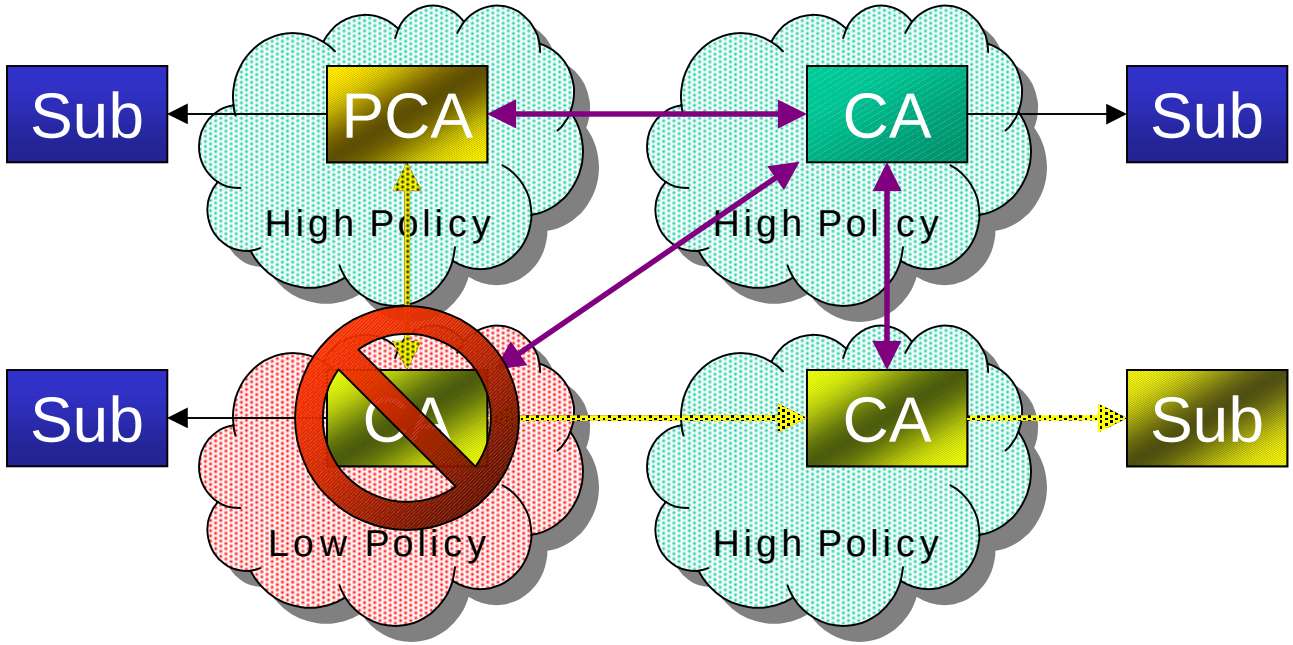
- In a mesh, it gets trickier… “follow the issuer” ends up with many choices.
- You might take a longer route…



Developing Certificate Paths in a Mesh (cont.)

CYGNACOM SOLUTIONS
an Entrust Technologies company

- In a mesh, it gets trickier… "follow the issuer" ends up with many choices.
- You might find invalid paths…

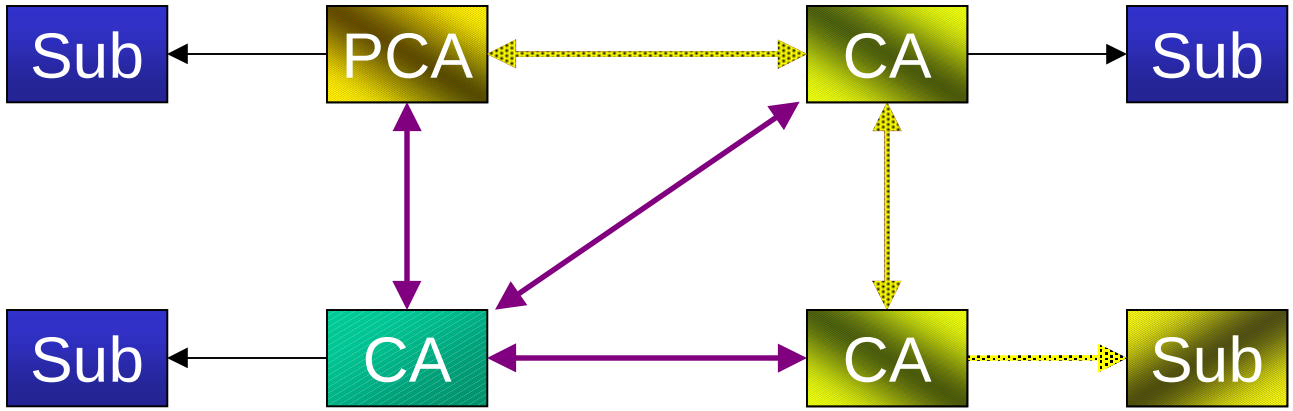


This slide is animated.

Developing Certificate Paths in a Mesh (cont.)

CYGNACOM SOLUTIONS
an Entrust Technologies company

- Perhaps a better method for finding your way through a mesh is top-down…



CYGNACOM SOLUTIONS
an Entrust Technologies company

Overview of CygnaCom's Path Development Software

Building a tool for Certificate Path Development

CYGNACOM SOLUTIONS
an Entrust Technologies company

- Don't
  - restrict the topology
  - rely on a specific repository access method
  - rely on a certificate/CRL caching method
  - miss any valid paths
  - depend on a specific operating system
- Do
  - function in a Bridge CA topology
  - optimize for speed whenever possible

Building a tool for Certificate Path Development

CYGNACOM SOLUTIONS
an Entrust Technologies company

- Certificate Path Development Library (CPL) Architecture
  - Windows DLL, written in ANSI C++
  - Uses caller-supplied callbacks for caching and directory retrieval
- Uses bottom-up (hierarchical) approach, with some enhancements to increase our likelihood of finding a valid path
    - Matching rules
    - Certificate Sorting
    - Policy checking (via ’97 X.509)

CPL Matching Rules

CYGNACOM SOLUTIONS
an Entrust Technologies company

- Uses keyUsage and subjectKeyID as matching criteria (if present)
- Ensures pathToName validates at every step
- Skips invalid (expired) certificates
- Allows specification of an acceptable list of algorithms
- If initial-inhibit-policy mapping is TRUE, ensures intersection of certificatePolicies and initial-acceptable-policy-set ≠ 0

CPL Certificate Sorting

CYGNACOM SOLUTIONS
an Entrust Technologies company

- We retrieve all certificates for each entity in the path during development
  - userCertificate
  - cACertificate
  - crossCertificatePair
- These certificates are sorted to help us find the “right” one fastest

CPL Certificate Sorting

CYGNACOM SOLUTIONS
an Entrust Technologies company

- Hierarchical certificates have priority over cross certificates
- Certificates with consistent public key and signing algorithms have priority
- Certificates that assert policies in the initial-acceptable-policy-set have priority
- Certificates that assert policies should have priority
- Certificates with fewer RDN elements in the Issuer DN have priority
- Certificates with most matching RDNs between the Issuer DN and trust root DN have priority
- Certificates with most matching RDNs between the Subject DN and the Issuer DN have priority
- Certificates with longer validity periods have priority

CYGNACOM SOLUTIONS
an Entrust Technologies company

Lessons Learned Developing and Testing Path Development Software

Lessons Learned

CYGNACOM SOLUTIONS
an Entrust Technologies company

- Directory population by CA products of cross-certificates is not always done completely/correctly
  - This is hard because the forward/reverse elements need to be encoded together and posted in two separate entries
  - LDAPv2 Schema only requires forward, some software requires both

Lessons Learned (cont.)

CYGNACOM SOLUTIONS
an Entrust Technologies company

- Directory logs can go a long way toward helping problems be diagnosed
  - You can see the retrieval requests in order
  - This helps you determine when the retrievals stopped, if retrievals started looping, etc.

Lessons Learned (cont.)

CYGNACOM SOLUTIONS
an Entrust Technologies company

- As you can already tell, the directory is the key to the path development process. Make sure…
  - you have access to good directory software
  - required information is in the directory
  - you have access to people that can help with directory operations

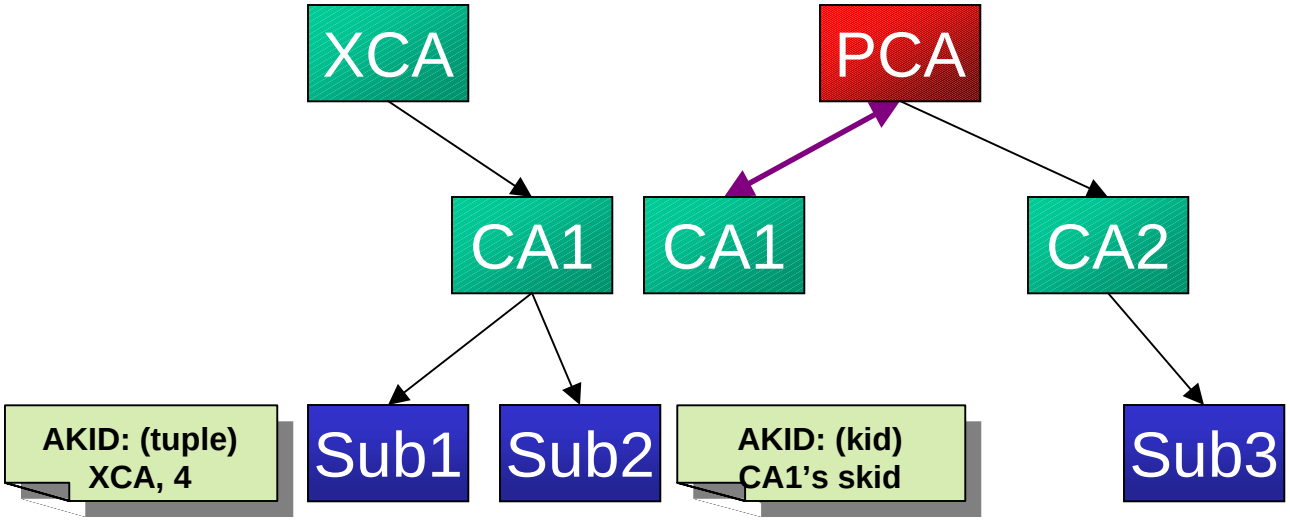
Lessons Learned (cont.)

CYGNACOM SOLUTIONS
an Entrust Technologies company

- authKeyID cannot be used as a matching rule when developing paths if the **`authorityCertIssuer`** and **`authorityCertSerialNumber`** tuple is used. (Explanation follows)
- We submitted this as a defect report to ISO/ITU to get it deprecated in later versions of X.509. The editors have decided to instead add clarifying text to X.509 (2000).

Authority Key Identifier Matching Rule Defect

CYGNACOM SOLUTIONS
an Entrust Technologies company



- Assuming Sub3's trust root is PCA, Sub3 will never find a path from Sub1 to PCA if AKID is used as a matching rule.
- However, Sub3 can find a path from Sub2 to PCA

CYGNACOM SOLUTIONS
an Entrust Technologies company

Other Path Development Software and Development Efforts

Other Path Development Software

CYGNACOM SOLUTIONS
an Entrust Technologies company

- As far as I know, the Entrust products are the only commercial software that can navigate complex trust paths such as these
- If I'm wrong and there are others, please let me know!
- Hopefully other commercial vendors will "jump on the bandwagon" soon

Other Development Efforts

CYGNACOM SOLUTIONS
an Entrust Technologies company

- The Sun Microsystems Java Community Process has just begun creation and review of the Java Certification Path API
- Sun Microsystems will be developing a reference implementation once the API is firm
- I encourage you all to join the community process and/or participate in the public comment and review of JSR-00055:

  http://java.sun.com/aboutjava/communityprocess

CYGNACOM SOLUTIONS
an Entrust Technologies company

Thanks for your time!

Contact me with any questions:

Peter Hesse
pmhesse@cygnacom.com
(703)848-0883